様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 １５ 日現在

機関番号：１３６０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2020
課題番号：１７Ｋ００１８２

研究課題名（和文）形式手法による暗号の安全性証明自動検証システムの開発

研究課題名（英文）Developing Automated formal Verification System for Cryptology

研究代表者
岡崎　裕之（Okazaki, Hiroyuki）

信州大学・学術研究院工学系・助教

研究者番号：５０４３２１６７

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：本研究では、形式的定理証明系Mizarとモデル検査器ProVerifを用いて、計算機援用による暗号システムの安全性形式的評価システムを開発した。
Mizarでは暗号理論に関わる形式化数学ライブラリを開発した。本成果は確率、統計、関数解析、計算アルゴリズムや計算量等の計算機科学の基礎の形式化であるので、暗号理論以外にも応用できる。
一方、ProVerifでは、基本的な暗号プロトコルのみならず、従来より抽象度が低くより現実のシステムや実装に近いモデルでの安全性検証手法を提案した。これにより暗号学的ハッシュ関数やブロック暗号の利用モード等の開発時の設計支援や形式的安全性検証を行うことが可能となった。

研究成果の学術的意義や社会的意義
本研究では、形式的定理証明系Mizarとモデル検査器ProVerifを用いて、実用的な計算機援用による暗号システムの安全性形式的評価システムの開発を行った。前者は主に暗号理論の専門家が安全性証明を行う際に、証明の正しさを計算機によって検証することに利用できる。後者は暗号理論の専門家ではないネットワークやIoT技術のような暗号技術の利用者が、セキュアなシステム開発の際に、正しく暗号技術を利用するための支援や暗号技術の学習に利用でき、いずれもSociety5.0の発展に貢献できるものである。

研究成果の概要（英文）：In this research, we developed a practical computer-assisted formal verification system for security of cryptographic systems using a formal theorem prover Mizar and a security model checker ProVerif. By using Mizar, we has developed formalized mathematical library related to cryptology. Since this result is a formalization of the basics of computer science such as probability, statistics, functional analysis, calculation algorithms and computational complexity, it can be applied to other than cryptology. On the other hand, by using ProVerif, we proposed a security verification method not only for basic cryptographic protocols but also for models suit for actual systems and implementations. Our proposed method has made it possible to provide design support and formal security verification during development of actual cryptographic modules such as cryptographic hash functions and block cipher modes of operation.

研究分野：情報セキュリティ

キーワード：暗号理論　形式的安全性検証　形式的定理証明　モデル検査　Mizar　ProVerif

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

計算機援用による暗号の安全性証明を形式的定理証明検証やモデル検査等の形式手法を用いて行う試みが当時より注目を集めていた。形式的定理証明検証とは定義や定理、証明を形式的言語で記述し、証明の正当性を計算機で自動的に検証する技術である。一方、モデル検査は計算機が自動的に行う技術であるが、専ら網羅探索による攻撃の発見に用いられる。そのため、モデル検査技術による暗号の安全性検証は暗号の設計には大変有効ではあるが、モデル検査によって全ての攻撃が発見されるわけではないので、形式的安全性検証の完全自動化は困難であった。

当該分野の他の類似するプロジェクト等では形式的自動安全性検証の実現を優先し大きな成果を上げてきたが、ほとんどの場合は特定のモデル上で既存の安全性証明を形式化し、その検証を自動化しただけで、既存の暗号方式やシステムに対する安全性検証・証明を形式手法を用いて再現もしくは別証明を与えるに留まっていた。そこで、新たな暗号の提案や、プロトコル設計時に実際に利用できる形式手法による安全性検証支援ツールが望まれていた。

２．研究の目的

本研究では暗号理論と形式的定理証明について双方の専門知識を駆使し、暗号研究者が通常行う証明と同様の方法、すなわち対象となる暗号の安全性を保証する数学的な定理証明を手動で記述し、その証明を検証するために形式的定理証明システム Mizar を利用するという極めて原始的な解決方針の下で安全性検証システムの実用化を進めた。本研究の成果を用いることにより、暗号理論で必要となる数学知識や最新の成果の全てを形式検証することが目的であった。本研究成果として公開する正当性の検証が計算機によってなされた一貫した統合ライブラリとして整備され、誰もが安全性証明の自動検証に利用可能なシステムを利用すれば、暗号研究者は自動検証により煩わしい場合分けや定理の適用の可否の判断を計算機に任せ、安全性証明の本質にのみ注力できると予想できる。

一方で、暗号技術はもはや専門家だけが研究・開発を行うものにとどまらず、ICT の基盤として Society5.0 実現の為に必要不可欠な技術となっている。そこで、モデル検査による暗号プロトコル安全性モデル検査器 ProVerif を併用することで IoT やネットワーク技術者などの暗号理論の非専門家にも利用可能な形式的安全性検証ツールの実用化が本研究の大目的であった。

３．研究の方法

本研究では形式的定理証明システム Mizar と暗号プロトコル安全性モデル検査器 ProVerif を併用することで、双方の利点を生かして、形式手法の専門知識がない暗号研究者にも利用可能な暗号の安全性形式的安全性検証システムを開発する。他の形式的定理証明システムを利用した先行研究の多くは既存の安全性証明方法を基にした暗号モデルを形式的に定義し、そのモデル上で定性的な安全性証明を形式化している。そのため新たな証明方法や、自動証明等の他のシステムとの連携にはモデルを作り直さなければならない。また、具体的な暗号プリミティブの評価は、先行研究では最初から想定されていない。そこで特定のモデル上で安全性証明を行うのではなく、通常の安全性証明そのものを形式言語で記述し、計算機援用による形式的定理証明検証の開発を進めた。本研究の準備として、暗号の安全性証明に必要となる確率論、計算量理論、整数論等の計算機科学、数学の多分野にまたがる緒定義、定理の形式化ライブラリを作成していた。本研究ではこれらのライブラリをさらに発展させて暗号理論のための形式化数学ライブラリを整備すること、および暗号理論の最先端の研究において利用可能なほど実用的な安全性証明の形式的検証システムの開発を行った。一方で、ProVerif を用いた暗号プロトコルの安全性モデル検査の高度化に取り組んでいる。通常、ProVerif では特定の攻撃を検出するクエリしか利用できないので ProVerif の検証結果は「攻撃が発見されなかった」という消極的な意味しか持ちえないが、本研究では、ある攻撃を ProVerif がサポートする攻撃に帰着する方法を提案し、この方法を利用して Mizar をはじめとする他の形式手法ツールとの連携をはかり、より実用的な計算機援用による暗号システムの安全性形式的評価システムの開発を進めた。

４．研究成果

暗号の安全性を形式的定理証明検証や形式的自動証明等の計算機援用による形式的評価を用いて行う試みが注目を集めている。本研究では、形式的定理証明系 Mizar 等を用いて、特定のモデルや証明方法に依存しない、汎用性の高い暗号理論に関わる基礎的な形式化数学ライブラリを開発することで、実用的な計算機援用による暗号システムの安全性形式的評価システムの開発を目的とする。

本研究では主に、(1)暗号理論で必要となる数学、および計算機科学に関する形式化ライブラリ開発、(2)モデル検査器による暗号プロトコルおよび暗号アルゴリズムに関する形式化の 2 つの方法で研究を進めた。

本研究成果とその分担を図 1 に示す。

(1)Mizar 暗号による理論で必要となる数学、および計算機科学に関する形式化ライブラリ開発

暗号理論、特に安全性証明の為に必要となる数理・情報分野は、統計、確率論やその基礎となる関数解析、アルゴリズムおよび計算量評価、数論等多岐にわたる。本研究では確率論、関数解析分野の形式化数学ライブラリ開発を研究分担者の師玉が、アルゴリズムおよび計算量、数論の形式化数学ライブラリ開発を研究分担者の布田と研究代表者岡崎が主に担当した。

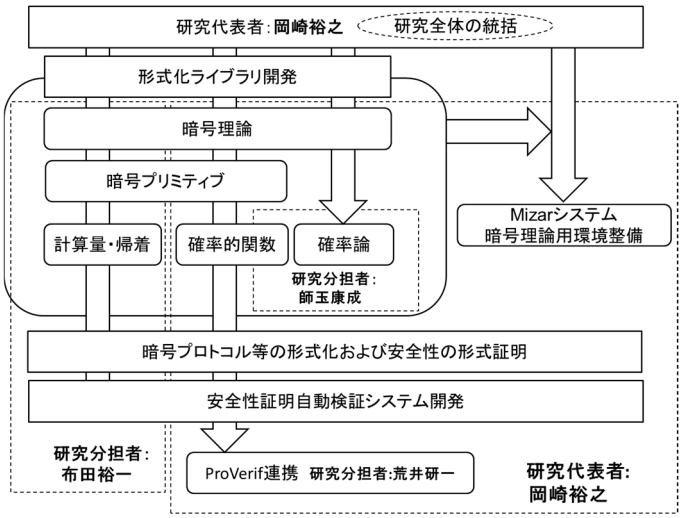

図 1：研究成果概要とその分担者

確率論および関数解析については、微分可能性、リプシッツ連続性等の形式化ライブラリを開発し、本研究開始時に既に完成していた離散確率分布のライブラリと合わせて攻撃可能性の評価や確率的アルゴリズムの形式化をさらに進めるための準備が進んでいる。

アルゴリズムと計算量の評価の形式化のための形式化については、単純ループ構造によるアルゴリズムの形式化、そのアルゴリズムの終了ステップ数やオーダー評価、計算問題間の帰着関係の形式化のための形式化手法の提案を行った。さらに提案手法の応用例として拡張ユークリッド互除法や高速べき乗演算等の暗号開発に必要となるアルゴリズムの形式化と最大ステップ数の評価に関する形式化ライブラリを開発した。

数論に関しては、暗号で利用されるより複雑なアルゴリズム評価の準備のために、アフィン座標上の楕円曲線演算、整数のバイナリ表現等に関する形式化数学ライブラリを開発した。

(2)モデル検査器 ProVerif による暗号プロトコルおよび暗号アルゴリズムに関する形式化

暗号プロトコルの安全性モデル検査器である ProVerif での暗号機能の形式化を行った。研究分担者の荒井、布田と研究代表者岡崎が主に担当した。特に繰り返しや関数呼び出しを含む暗号モジュールの実装技術の安全性検証方法に関する提案、評価を行った。

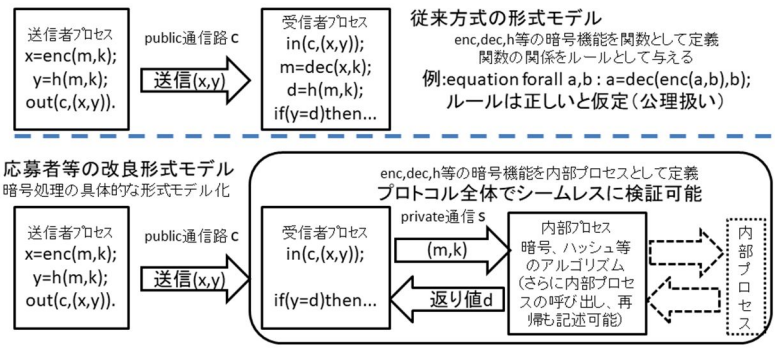

図 2：PrVerif による実装の形式化

ProVerif をはじめとするモデル探索による暗号プロトコル安全性検証ツールでは、抽象度の低い実装に即した安全性検証を行うことは困難であったが、本研究で提案した検証手法（図 2）により、暗号学的ハッシュ関数の構成法として知られる MD 変換やスポンジ構造、CBC モードに代表される秘密鍵暗号の利用モード等の形式モデル化と安全性検証を実現した。

さらに本研究成果の一部を利用した暗号プロトコルに関する教育の試みが、第 5 回 実践的 IT 教育シンポジウム rePiT2019 in 愛媛（ソフトウェア科学会、enPit2 共催）において優秀教育実践賞を受賞した。この取り組みは教育工学の研究として基盤研究(C)18K02917 ”情報セキュリティ人材育成のための暗号技術学習支援 e ラーニングシステムの開発（代表：村上 恭通）”に引き継がれ、岡崎及び布田が研究分担者として参加している。

本研究の目的は、計算機援用による実用的な形式的安全性検証システムの開発であった。そのため、本研究で開発した安全性検証システムを実際の製品開発に利用されることが、本研究の真の成果になると考える。そこで計算機援用による暗号技術を利用したシステムやプロトコルの設計および安全性検証を支援するツールの開発とその普及は有意義である。そこで、本研究の成果の一部を用いて、民間企業との共同研究で IoT 機器を利用したセキュアなシステム設計に特化した安全性検証支援ツールとしての実用化フェーズの研究を始めている。さらに暗号システム以外の安全性検証へ本研究の応用範囲を広げるために、ネットワークセキュリティ分野においても学内および学外の研究者との共同研究を進めている。

今後、本研究の成果をはじめとする計算機援用による形式的安全性検証技術を ICT 技術全般の開発段階において利用できるようになれば、Society5.0 実現に大きく貢献できると考える。

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　0件／うちオープンアクセス　10件）

１．著者名 Yamazaki Hiroshi, Miyajima Keiichi, Shidama Yasunari	４．巻 29
２．論文標題 Functional Space Consisted by Continuous Functions on Topological Space	５．発行年 2021年
３．雑誌名 Formalized Mathematics	６．最初と最後の頁 51～65
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2021-0005	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Nakasho Kazuhisa, Futa Yuichi	４．巻 29
２．論文標題 Inverse Function Theorem. Part I	５．発行年 2021年
３．雑誌名 Formalized Mathematics	６．最初と最後の頁 9～20
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2021-0002	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Nakasho Kazuhisa, Shidama Yasunari	４．巻 27
２．論文標題 Continuity of Multilinear Operator on Normed Linear Spaces	５．発行年 2019年
３．雑誌名 Formalized Mathematics	６．最初と最後の頁 61～65
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2019-0006	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Nakasho Kazuhisa, Shidama Yasunari	４．巻 27
２．論文標題 Implicit Function Theorem. Part II	５．発行年 2019年
３．雑誌名 Formalized Mathematics	６．最初と最後の頁 117～131
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2019-0013	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Okazaki Hiroyuki, Nagao Koh-ichi, Futa Yuichi	4．巻 27
2．論文標題 Maximum Number of Steps Taken by Modular Exponentiation and Euclidean Algorithm	5．発行年 2019年
3．雑誌名 Formalized Mathematics	6．最初と最後の頁 87～91
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2019-0009	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Futa Yuichi, Okazaki Hiroyuki, Shidama Yasunari	4．巻 27
2．論文標題 Operations of Points on Elliptic Curve in Affine Coordinates	5．発行年 2019年
3．雑誌名 Formalized Mathematics	6．最初と最後の頁 315～320
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2019-0026	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 岡崎 裕之，紫村 彰吾，宮本 樹，渡邊 樹，布田 裕一，村上 恭通	4．巻 37
2．論文標題 形式的安全性検証ツールを用いた暗号教育の実践とそのe-Learning教材化の課題について	5．発行年 2020年
3．雑誌名 コンピュータ ソフトウェア	6．最初と最後の頁 99～113
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_99	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Okazaki Hiroyuki	4．巻 26
2．論文標題 Binary Representation of Natural Numbers	5．発行年 2018年
3．雑誌名 Formalized Mathematics	6．最初と最後の頁 223～229
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2018-0020	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Nakasho Kazuhisa, Futa Yuichi, Shidama Yasunari	4．巻 26
2．論文標題 Continuity of Bounded Linear Operators on Normed Linear Spaces	5．発行年 2018年
3．雑誌名 Formalized Mathematics	6．最初と最後の頁 231～237
掲載論文のDOI（デジタルオブジェクト識別子） 10.2478/forma-2018-0021	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Nakasho Kazuhisa, Futa Yuichi, Shidama Yasunari	4．巻 25
2．論文標題 Implicit Function Theorem. Part I	5．発行年 2017年
3．雑誌名 Formalized Mathematics	6．最初と最後の頁 269～281
掲載論文のDOI（デジタルオブジェクト識別子） 10.1515/forma-2017-0026	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計20件（うち招待講演　1件／うち国際学会　5件）

1．発表者名 五十嵐 孝洋，布田 裕一
2．発表標題 ブロックチェーンとフォグノードを用いたIoT機器の認証・認可
3．学会等名 電子情報通信学会,ICSS研究会
4．発表年 2021年

1．発表者名 原田 雄基，布田 裕一，岡崎 裕之
2．発表標題 制御システムにおける異常検知手法とデータセットの評価
3．学会等名 2021年暗号と情報セキュリティシンポジウム（SCIS2021）
4．発表年 2021年

１．発表者名
吉村 東悟，荒井 研一，岡崎 裕之，布田 裕一，三重野 武彦

２．発表標題
ProVerifを用いたスポンジ構造の形式化

３．学会等名
2021年暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
吉村 東悟，荒井 研一，岡崎 裕之，布田 裕一，三重野 武彦

２．発表標題
ProVerifを用いたMD変換の形式化

３．学会等名
日本応用数理学会 2020年度 年会

４．発表年
2020年

１．発表者名
Tokuyama Ryo, Futa Yuichi, Suzuki Hikofumi, Okazaki Hiroyuki

２．発表標題
Virtual Environment for Analysis and Evaluation of DDoS Attacks

３．学会等名
INTRICATE-SEC-2021, Proceedings of the 35th International Conference on Advanced Information Networking and Applications(AINA-2021)（国際学会）

４．発表年
2021年

１．発表者名
Mieno Takehiko, Yoshimura Togo, Hiroyuki Okazaki, Yuichi Futa, Kenichi Arai

２．発表標題
Formal Verification of Merkle-Damgard Construction in ProVerif

３．学会等名
The International Symposium on Information Theory and Its Applications(ISITA2020)（国際学会）

４．発表年
2020年

１．発表者名
Yoshimura Togo, Arai Kenichi, Okazaki Hiroyuki, Futa Yuichi

２．発表標題
Formalization of Security Requirements and Attack Models for Cryptographic Hash Functions in ProVerif

３．学会等名
ProVerif,The 2019 International Conference on Security and Management (SAM'19) (国際学会)

４．発表年
2019年

１．発表者名
岡崎 裕之，布田 裕一，師玉 康成

２．発表標題
Mizarによる離散確率分布の統計的識別不能性の形式化

３．学会等名
日本応用数理学会 2019年度 年会

４．発表年
2019年

１．発表者名
吉村 東悟，荒井 研一，岡崎 裕之，布田 裕一，三重野 武彦

２．発表標題
ProVerifを用いたMD変換の形式化

３．学会等名
2020年暗号と情報セキュリティシンポジウム（SCIS2020）

４．発表年
2020年

１．発表者名
高橋 幸宏，布田 裕一，岡崎 裕之，鈴木 彦文

２．発表標題
協調型DNSによるキャッシュポイズニングの検知

３．学会等名
2020年暗号と情報セキュリティシンポジウム（SCIS2020）

４．発表年
2020年

１．発表者名
磯貝 百恵，岡崎 裕之，荒井 研一，布田 裕一，三重野 武彦

２．発表標題
モデル検査器ProVerifによるDES暗号の形式化

３．学会等名
2020年電子情報通信学会総合大会

４．発表年
2020年

１．発表者名
荒井 研一，岡崎 裕之，布田 裕一

２．発表標題
ProVerifを用いたCT及びブロックチェーンの形式化

３．学会等名
2019年暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
渡邊 樹，宮本 樹，紫村 彰吾，岡崎 裕之，布田 裕一，村上 恭通

２．発表標題
Moodleを用いたProverifのeラーニングシステム

３．学会等名
第41回情報理論とその応用シンポジウム(SITA2018)，Poster session

４．発表年
2018年

１．発表者名
Miyamoto Tatsuki, Shimura Shogo, Watanabe Tatsuki, Okazaki Hiroyuki, Futa Yuichi, Murakami Yasuyuki

２．発表標題
e-Learning System for Cryptography on Moodle

３．学会等名
Internet Conference 2018 (IC2018),Poster session（国際学会）

４．発表年
2018年

１．発表者名
荒井 研一，岡崎 裕之，布田 裕一

２．発表標題
ProVerif を 用いたTLS1.3ハンドシェイクプロ トコルの形式検証

３．学会等名
日本応用数理学会 2018年度 年会（招待講演）

４．発表年
2018年

１．発表者名
Okazaki Hiroyuki, Futa Yuichi, Arai Kenichi

２．発表標題
Suitable Symbolic Models for Cryptographic Verification of Secure Protocols in ProVerif

３．学会等名
The International Symposium on Information Theory and Its Applications(ISITA2018)（国際学会）

４．発表年
2018年

１．発表者名
紫村 彰吾，岡崎 裕之，宮本 樹，渡邊 樹，布田 裕一，村上 恭通

２．発表標題
形式的安全性検証ツールを用いた暗号教育の実践とそのe-Learning教材化の課題について

３．学会等名
第5回 実践的IT教育シンポジウム rePiT2019 in 愛媛

４．発表年
2019年

１．発表者名
田付 洋大，布田 裕一，鈴木 智道，田中 覚

２．発表標題
CAN-Ethernet変換における不正アクセスの検知

３．学会等名
情報処理学会 第81回全国大会

４．発表年
2019年

１．発表者名 荒井 研一，岡崎 裕之，布田 裕一
２．発表標題 ProVerifにおける暗号プリミティブの安全性要件と攻撃モデルの形式化方法について
３．学会等名 日本応用数理学会2017年度 年会
４．発表年 2017年

１．発表者名 荒井 研一，岡崎 裕之，布田 裕一
２．発表標題 ProVerifを用いたCTの形式化
３．学会等名 2018年 暗号と情報セキュリティシンポジウム（SCIS2018）
４．発表年 2018年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称 IoTデバイス間での相互認証付き鍵共有システム	発明者 三重野 武彦，岡崎 裕之	権利者 同左
産業財産権の種類、番号 特許、特願２０２０－２０４３７１	出願年 2020年	国内・外国の別 国内

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	布田　裕一 (Futa Yuichi) (50706223)	東京工科大学・コンピュータサイエンス学部・准教授 (32692)	
研究分担者	師玉　康成 (Shidama Yasunari) (20226129)	信州大学・学術研究院工学系・教授 (13601)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	荒井　研一 (Arai Kenichi) (60645290)	長崎大学・工学研究科・助教 (17301)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関